



Contribution ID: 84

Type: **Poster presentation**

Software Integrity Analysis Applied to IRIO EPICS Device Support Based On FPGA Real-Time DAQ Systems

Tuesday 7 June 2016 15:00 (1h 30m)

Nuclear fusion environments require dependability and safety analysis to ensure a reliable design and a deterministic behaviour. Failure modes identification, risk assessment and mitigation, guarantee that quality control procedures at different architectural levels comply with all the well-defined prerequisites at all the commissioning stages. Therefore, exhaustive analysis based on Reliability, Availability, Maintainability and Safety (RAMS) must be an unavoidable activity in such a kind of undertaking. The results of this analysis impacts on the hardware and software development: invalidating inadequate software architectures and hardware components, and forcing a given development assurance level depending on its criticality (and thus its costs). This paper applies RAM analysis methodology for an advanced Data Acquisition System (DAQ) based on FPGA, using standards and techniques commonly used for critical systems developments.

The proposed DAQ system interfaces with signals coming from different sensors, acquiring data at high sampling rates (up to hundreds of MS/s), and in some cases performing Real-Time pre-processing. In turn, it must provide acquired data to control system, where control loopback will be applied. This fact implies that the DAQ system shall guarantee integrity, continuity, availability and accuracy, providing with the necessary integrity level.

This paper presents the analysis for the IRIO software tools as part of an EPICS IOC running under a hardware architecture compliant with the ITER catalogue for fast controllers. This analysis focuses on: RAM analysis to ensure the technical risk control and mitigation; criticality analysis and assessment of mixed-critical systems for failure propagation mitigation by the usage of segregation strategies, such as virtualization techniques by using hypervisors; the IRIO Software Integrity Level (SWIL) analysis, according to nuclear critical system requirements; and software verification methodology based on source code static analysis to reduce errors present in the final product. This analysis will provide confident methodologies to to be considered in future software implementations for minimizing costs and risks in such kind of nuclear environments.

Author: Dr SANZ, Diego (GMV)

Co-authors: Mr BUSTOS, Alvaro (GMV); Mr AUTRÁN, Joaquín (GMV); Prof. RUIZ, Mariano (Universidad Politecnica de Madrid); Ms FERNÁNDEZ, Marta (GMV); Dr URUEÑA, Santiago (GMV); Mr ESQUEMBRI, Sergio (Universidad Politecnica de Madrid)

Presenter: Dr SANZ, Diego (GMV)

Session Classification: Poster session 1